UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Information associated with the Dropbox accounts littleboysunder@yahoo.com, lovepics9@yahoo.com, lovepics9@aol.com, and johnadams1.9@yahoo.com

Case No. 3:18mj164

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:
See Attachment A-5

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:
See Attachment B-5

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
See Attachment C-5	

The application is based on these facts:
See Attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of ____ days (give exact ending date if more than 30 days: ____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Andrea R. Kinzig

Applicant's signature

Andrea R. Kinzig, Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 3-2-18

Sharon L. Ovington

Judge's signature

City and state: Dayton, Ohio

Sharon L. Ovington, U.S. Magistrate Judge

Printed name and title

ATTACHMENT A-5

Property to Be Searched

Information associated with the Dropbox accounts associated with the email addresses **littleboysunder@yahoo.com**, **lovepics9@yahoo.com**, **lovepics9@aol.com**, and **johnadams1.9@yahoo.com** that is stored at premises owned, maintained, controlled, or operated by Dropbox Inc., a company that accepts service of legal process at 185 Berry Street, Suite 400, San Francisco, California, 94107.

ATTACHMENT B-5

Particular Things to be Seized

I. Information to be disclosed by Dropbox Inc. (the "Provider")

To the extent that the information described in Attachment A-5 is within the possession, custody, or control of the Provider, including any records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A-5:

a. All available user/subscriber details for the account, including: full name, user identification number, birth date, gender, contact e-mail addresses, passwords, security questions and answers, telephone numbers, screen names, websites, and other personal identifiers;

b. All files downloaded and/or uploaded by the user account, including any deleted files;

c. All activity logs for the account, including but not limited to auth.txt logs, uploag.html files, report.txt files, links.txt files, and any logs reflecting the deletion of files;

d. Records of any Dropbox links posted by the account user, and records of any other users who accessed these links;

e. Records of any Dropbox links accessed by the account user, and records of the original poster of those links;

f. All information related to the account's settings, including but not limited to linked devices, linked Facebook and Twitter accounts, etc.;

g. The length of service (including start date);

h. Any payment information related to the account, including full credit card numbers.

Notwithstanding 18 U.S.C. § 2252/2252A or any similar statute or code, Dropbox Inc. shall disclose responsive data by sending it to the Federal Bureau of Investigation at 7747 Clyo Road, Centerville, Ohio, 45459.

II. Information to be seized by the government

Items evidencing violations of 18 U.S.C. §§ 18 U.S.C. §2251(d) (advertisement of child pornography); 18 U.S.C. §§ 2252(a)(2)(B) and (b)(1) and 2252A(a)(2) and (b)(1) (receipt and attempted receipt of child pornography); 2252(a)(4)(B) and (b)(1) and 2252A(a)(5)(B) and (b)(1) (possession and attempted of child pornography); and 18 U.S.C. §2423(b) and (e) (travel or attempted travel in interstate commerce with the intent to engage in illicit sexual conduct), including but not limited to the following:

a. Any visual depictions and records related to the possession, receipt, and advertisement of child pornography and the travel with the intent to engage in illicit sexual conduct;

b. Any visual depictions of minors and any associated contact information for these minors and their guardians;

c. Any information regarding child pornography files shared with others;

d. Evidence of utilization of aliases and fictitious names;

e. Evidence of utilization of the account names boysunder9, Bigman23, Littledicklover, and Babyboys.

f. Any records or other information related to the possession, receipt, and advertisement of child pornography and the travel with the intent to engage in illicit sexual conduct;

g. Any information related to Internet Protocol (IP) addresses accessed by the account;

h. Information relating to who created, used, or communicated with the account, including records about their identities and whereabouts.

ATTACHMENT C-5

Code Section	Offense Description
18 U.S.C. §2252(a)(4)(B) & (b)(1)	Possession or Attempted Possession of Child Pornography
18 U.S.C. §2252A(a)(5)(B) & (b)(1)	Possession or Attempted Possession of Child Pornography
18 U.S.C. §2252(a)(2)(B) & (b)(1)	Receipt or Attempted Receipt of Child Pornography
18 U.S.C. §2252A(a)(2) & (b)(1)	Receipt or Attempted Receipt of Child Pornography
18 U.S.C. §2251(d)	Advertisement of Child Pornography
18 U.S.C. §2423(b) & (e)	Travel or Attempted Travel with Intent to Engage in Illicit Sexual Activity

AFFIDAVIT IN SUPPORT OF SEARCH WARRANTS

I, Andrea R. Kinzig, being duly sworn, depose and state the following:

INTRODUCTION

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), and have been so employed since 2005. I am currently assigned to the Dayton, Ohio Resident Agency of the Cincinnati Field Office. In connection with my official duties, I investigate violations of federal criminal laws, including offenses pertaining to the illegal production, distribution, receipt, and possession of child pornography (in violation of 18 U.S.C. §§ 2252(a) and 2252A) and coercion and enticement (in violation of 18 U.S.C. §2422). I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in various forms of media, including computer media.

2. Along with other agents and investigators of the FBI, I am currently involved in an investigation of child exploitation offenses committed by TYLER ULM. This Affidavit is submitted in support of Applications for search warrants for the following:

   a. Information associated with the Google accounts **tylerjulm22@gmail.com, tylerjulm@gmail.com,** and **damonvaughn0@gmail.com** that is stored at premises controlled by Google Inc. (as more fully described in Attachment A-1);

   b. Information associated with the email accounts **lovepics9@yahoo.com, d9underboy@yahoo.com, kids9nunder@yahoo.com, littleboysunder@yahoo.com, johnadams1.9@yahoo.com, tylerjulm@yahoo.com,** and **omkexddwbkit3s2eatevv5zx3bne75kjo4kfarxo@yahoo.com** and the Flickr NSID's **146969803@N06, 150137400@N03, 146772605@N03, 145287374@N02, 161195535@N07,** and **147418551@N04** that is stored at premises controlled by Oath Holdings Inc. (as more fully described in Attachment A-2);

   c. Information associated with the email accounts **ahopping0406@aol.com** and **lovepics9@aol.com** that is stored at premises controlled by Oath Inc. (as more fully described in Attachment A-3);

   d. Information associated with the Facebook User ID **Tyler.Ulm.7** that is stored at premises controlled by Facebook Inc. (as more fully described in Attachment A-4);

   e. Information associated with the Dropbox accounts associated the email addresses **littleboysunder@yahoo.com, lovepics9@yahoo.com, lovepics9@aol.com,** and

johnadams1.9@yahoo.com that is stored at premises controlled by Dropbox Inc. (as more fully described in Attachment A-5).

3. The purpose of the Applications is to seize evidence of violations of 18 U.S.C. §§ 2252(a)(4)(B) and (b)(1) and 2252A(a)(5)(B) and (b)(1), which make it a crime to possess or attempt to possess child pornography; violations of 18 U.S.C. §§ 2252(a)(2)(B) and (b)(1) and 2252A(a)(2) and (b)(1), which make it a crime to receive or attempt to receive child pornography through interstate commerce; violations of 18 U.S.C. § 2251(d), which make it a crime to advertise child pornography; and violations of 18 U.S.C. § 2423(b) and (e), which make it a crime to travel or attempt to travel in interstate commerce with the intent to engage in illicit sexual conduct. The items to be searched for and seized are described more particularly in Attachments B-1 through B-5 hereto.

4. As part of the investigation, I have reviewed documentation and reports provided by and discussed information with other agents and investigators involved in the investigation. For purposes of this Affidavit, I have not distinguished between information of which I have direct knowledge and that of which I have hearsay knowledge.

5. This Affidavit does not contain every fact known to the investigation, but only those deemed necessary to demonstrate sufficient probable cause to support the searches of the above noted accounts (as described in Attachments A-1 through A-5).

6. As a result of the instant investigation described more fully below, there is probable cause to believe that evidence, fruits, and instrumentalities of violations of federal law, including 18 U.S.C. §§ 2252(a)(4)(B) and (b)(1), 2252A(a)(5)(B) and (b)(1), 2252(a)(2)(B) and (b)(1), 2252A(a)(2) and (b)(1), 2251(d), and 2423(b) and (e), are present within the information associated with the above noted accounts (as described in Attachments A-1 through A-5).

JURISDICTION

7. This court has jurisdiction to issue the requested warrants because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

BACKGROUND INFORMATION

Pertinent Federal Statutes

8. 18 U.S.C. § 2251(d) states that it is a violation for (1) any person to knowingly make, print, or publish, or cause to be made, printed, or published, any notice or advertisement seeking or offering: (A) to receive, exchange, buy, produce, display, distribute, or reproduce any visual depiction, if the production of such visual depiction involves the use of a minor

engaging in sexually explicit conduct and such visual depiction is of such conduct; or (B) participation in any act of sexually explicit conduct by or with any minor for the purpose of producing a visual depiction of such conduct; (2) if such person knows or has reason to know that such notice or advertisement will be transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means including by computer or mailed; or such notice or advertisement is transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means including by computer or mailed.

9. 18 U.S.C. § 2252(a)(2)(B) and (b)(1) states that it is a violation for any person to knowingly receive or distribute any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, shipped, or transported in or affecting interstate or foreign commerce or which contains materials which have been mailed or so shipped or transported by any means, including by computer, or to knowingly reproduce any visual depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mails if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct, or attempt to do so.

10. 18 U.S.C. § 2252A(a)(2) and (b)(1) states that it is a violation for any person to receive or distribute – (A) any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; and (B) any material that contains child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer, or attempt to do so.

11. 18 U.S.C. § 2252(a)(4)(B) and (b)(1) states that it is a violation for any person to knowingly possess, or knowingly access with the intent to view, one or more matters which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct, or attempt to do so.

12. 18 U.S.C. § 2252A(a)(5)(B) and (b)(1) states that it is a violation for any person to knowingly possess, or knowingly access with intent to view, any book, magazine, periodical, film, videotape, computer, disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, that was produced using materials that have been

mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer, or attempt to do so.

13. For purposes of these statutes, the term "sexually explicit conduct" is defined in 18 U.S.C. § 2256(2) as:

a. "Actual or simulated –

i. Sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex;
ii. Bestiality;
iii. Masturbation;
iv. Sadistic or masochistic abuse; or
v. Lascivious exhibition of genitals or pubic area of any person."

14. 18 U.S.C. § 2423(b) and (e) states that it is a violation for any person to travel in interstate commerce or travel into the United States, or a United States citizen or an alien admitted for permanent residence in the United States to travel in foreign commerce, for the purpose of engaging in any illicit sexual conduct with another person, or attempt to do so.

Definitions

15. The following definitions apply to this Affidavit and Attachments B-1 through B-5 to this Affidavit:

a. "**Child Pornography**" includes the definition in Title 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).

b. "**Visual depictions**" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image (see 18 U.S.C. § 2256(5)).

c. "**Minor**" means any person under the age of eighteen years (see 18 U.S.C. § 2256(1)).

d. "**Sexually explicit conduct**" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the

same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person (see 18 U.S.C. § 2256(2)).

e. "**Internet Service Providers**" or "**ISPs**" are commercial organizations which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth that the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an e-mail address, and an e-mail mailbox, and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and password.

f. An "**Internet Protocol address**", also referred to as an "**IP address**", is a unique numeric address that computers or electronic devices use in order to communicate with each other on a computer network utilizing the Internet Protocol (IP) standard. Every computer or device connected to the Internet is referenced by a unique IP address. An IP address can be thought of as the equivalent to a street address or a phone number, just as each street address and phone number uniquely identifies a building or telephone. IP addresses are composed of four sets of digits known as "octets," ranging in value from 0-255, separated by decimal points. An example of an IP address is 192.168.10.102. There are two types of IP addresses; static and dynamic. A static address is permanently assigned to a particular device and as a practical matter never changes. A dynamic address provided by an Internet service provider to a client computer is valid only for the duration of the session that the client computer is connected to the Internet (or other network).

g. A network "**server**," also referred to as a "**host**," is a computer system that has been designated to run a specific server application or applications and provide requested services to a "client" computer. A server can be configured to provide a wide variety of services over a network, including functioning as a web server, mail server, database server, backup server, print server, FTP (File Transfer Protocol) server, DNS (Domain Name System) server, to name just a few.

h. A "**client**" is the counterpart of a server or host. A client is a computer system that accesses a remote service on another computer by some kind of network. Web browsers (like Internet Explorer or Safari) are clients that connect to web servers and

retrieve web pages for display. E-mail clients (like Microsoft Outlook or Eudora) retrieve their e-mail from their Internet service provider's mail storage servers.

i. "**Domain Name**" refers to the common, easy to remember names associated with an IP address. For example, a domain name of "www.usdoj.gov" refers to the IP address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards – from right to left – further identifies parts of an organization. Examples of first level, or top level domains are typically ".com" for commercial organizations, ".gov" for the governmental organizations, ".org" for organizations, and, ".edu" for educational organizations. Second level names will further identify the organization, for example "usdoj.gov" further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov identifies the World Wide Web server located at the United States Department of Justice, which is part of the United States government. The Domain Name System, also referred to DNS, is a system of servers connected to each other using a common system of databases that resolve a particular domain name, such as "www.usdoj.gov," to its currently assigned IP address (*i.e.*, 149.101.1.32), to enable the follow of traffic across the Internet.

j. "**Log Files**" are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

k. "**Hyperlink**" (often referred to simply as a "link") refers to a navigation element in a web page or document that automatically brings the referred information (a.k.a. "resource") to the user when the navigation element is selected by the user. Hyperlinks are part of the foundation of the World Wide Web, but are not limited to a website for HTML.

l. "**Website**" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

m. "**Uniform Resource Locator**" or "**Universal Resource Locator**" or "**URL**" is the unique address for a file that is accessible on the Internet. For example, a common

way to get to a website is to enter the URL of the website's home page file in the Web browser's address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.

n. A "**Smartphone**" is a mobile cellular telephone that performs many of the functions of a computer, typically having a touchscreen interface, Internet access, and an operating system capable of running downloaded applications.

o. **Wi-Fi** is a technology that allows electronic devices to connect to a wireless LAN network. Devices that use Wi-Fi technology include personal computers, video game consoles, smartphones, digital cameras, tablets, and modern computers.

p. The terms "**records**," "**documents**," and "**materials**," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

Characteristics of Collectors of Child Pornography

16. Based upon my knowledge, training, and experience in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the collection of child pornography (hereafter "collectors"):

a. Collectors may receive sexual stimulation and satisfaction from contact with children, or from having fantasies of children engaged in sexual activity or suggestive poses, or from literature describing such activity.

b. Collectors may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Collectors typically use these materials for their

own sexual arousal and gratification. Collectors often have companion collections of child erotica. Child erotica are materials or items that are sexually suggestive and arousing to pedophiles, but which are not in and of themselves obscene or pornographic. Such items may include photographs of clothed children, drawings, sketches, fantasy writings, diaries, pedophilic literature and sexual aids.

c. Collectors who also actively seek to engage in sexual activity with children may use these materials to lower the inhibitions of a child they are attempting to seduce, convince the child of the normalcy of such conduct, sexually arouse their selected child partner, or demonstrate how to perform the desired sexual acts.

d. Collectors almost always possess and maintain their "hard copies" of child pornographic images and reference materials (*e.g.*, mailing and address lists) in a private and secure location. With the growth of the Internet and computers, a large percentage of most collections today are in digital format. Typically these materials are kept at the collector's residence for easy access and viewing. Collectors usually place high value on their materials because of the difficulty, and legal and social danger, associated with acquiring them. As a result, it is not uncommon for collectors to retain child pornography for long periods of time, even for years. Collectors often discard child pornography images only while "culling" their collections to improve their overall quality.

e. Collectors also may correspond with and/or meet others to share information and materials. They may save correspondence from other child pornography distributors/collectors, including contact information like email addresses, and may conceal such correspondence as they do their sexually explicit material.

f. Collectors prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

g. Subscribers to websites that are primarily designed to provide child pornography have a strong likelihood of being collectors of child pornography. This high degree of correlation between subscription and collection behavior has been repeatedly confirmed during several recent nationwide law enforcement initiatives.

Use of Computers and the Internet with Child Pornography

17. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other, as well the methods that individuals will use to interact with and sexually exploit children. Computers serve four

functions in connection with child pornography: production; communication; distribution and storage.

a. **Production**: Pornographers can now produce both still and moving images directly from a common video camera. The camera is attached, using a cable, directly to the computer using a device called a video capture board. This device turns the video output into a form that is usable by computer programs. The output of the video camera can be stored, manipulated, transferred or printed directly from the computer. The captured image can be edited (*i.e.*, lightened, darkened, cropped, digitally enhanced, *etc*.) with a variety of commonly available graphics programs. The producers of child pornography can also use scanners to convert hard-copy photographs into digital images.

b. **Communication**. Previously, child pornography collectors had to rely on personal contact, U.S. mail, and telephonic communications in order to sell, trade, or market pornography. Today most communications associated with the trafficking of child pornography occur via the obscurity and relative anonymity of the Internet. A device known as a modem allows any computer to connect to the Internet via telephone lines or broadband Internet connections. Once connected to the Internet, individuals search for and/or offer to distribute child pornography in a wide variety of ways. Many individuals congregate in topic-based Internet chat rooms implicitly or explicitly dedicated to child pornography. Online discussions in these chat rooms are usually done via instant message (or "IM"), and individuals may then establish one-on-one chat sessions involving private messages (or "PMs"), visible only to the two parties, to trade child pornography. These child pornography images may be attachments to the PMs, or they may be sent separately via electronic mail between the two parties. Pedophile websites communicate advertisements for the sale of child pornography, and individuals may order child pornography from these websites using email or send order information from their web browser (using HTTP computer language). Some individuals communicate via Internet Relay Chat (IRC) to discuss and trade child pornography images. It is not uncommon for child pornography collectors to engage in mutual validation of their interest in such material through Internet-based communications.

c. **Distribution**. Computers and the Internet are the preferred method to distribute child pornography. As discussed above, such images may be distributed via electronic mail (either as an attachment or embedded image), or through instant messages as attachments. Child pornography is regularly downloaded from servers or Usenet newsgroups via a method known as FTP (file transfer protocol). Child pornography images are also distributed from websites via client computers web browsers downloading such images via HTTP (Hyper Text Transfer Protocol). Peer-to-peer networks such as LimeWire and Gnutella are an increasingly popular method by which child pornography images are distributed over the Internet.

d. **Storage**. The computer's capability to store images in digital form makes it an ideal repository for pornography. A single floppy disk can store dozens of images and hundreds of pages of text. The size of computer hard drives used in home computers has grown tremendously within the last several years. Hard drives with the capacity of two hundred (200) gigabytes are not uncommon. These drives can store thousands of images at very high resolution. Remote storage of these images on servers physically removed from a collector's home computer adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and save that image to storage in another country. Once this is done, there is no readily apparent evidence at the scene of the crime. Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

Google Services

18. Google Inc. is a multi-national corporation with its headquarters located in Mountain View, California. The company specializes in Internet-related products and services, including an Internet search engine (www.google.com), productivity tools such as email service (gmail), and enterprise products such as Google Search Appliance.

19. Google Photos is a photograph and video sharing and storage service provided by Google Inc., located at photos.google.com. It allows users to back-up their photographs and videos so they can be accessed on any telephone, tablet, or computer. It also allows users to pool their photographs and videos together with others into shared albums. Photographs and videos can be organized and searched by places and things in them.

20. Google+ is a social networking and identity service website owned and operated by Google Inc., located at www.plus.google.com. Common features include the following:

a. Profiles: Users can establish profile pages to maintain personal information, similar to the Facebook and MySpace social networking sites.

b. Circles: Google+ allows users to establish "circles", which enables them to organize people into groups for sharing across various Google products and services. This service replaces the typical "Friends" list function used by sites such as Facebook and MySpace.

c. Communities: Communities allow users with common interests to communicate with each other.

d. Photos: Google+ allows users to post, back-up, and share photographs. Users can also make comments on photographs posted by other users.

e. Hangouts: Hangouts are places used to facilitate group video chat. Only Google+ users can join such chats.

f. Messenger: Messenger is a feature available to Android, iPhone, and SMS devices for communicating through instant messaging within Circles.

21. Google Web and App History is a feature of Google Search in which a user's search queries and results and activities on other Google services are recorded. The feature is only available for users logged into a Google account. A user's Web and App History is used to personalize search results with the help of Google Personalized Search and Google Now.

22. Google Drive is a file storage and synchronization service provided by Google Inc., located at www.drive.google.com. This service provides cloud storage, file sharing, and collaborative editing capabilities. It offers 15 GB of online storage space, which is usable across Google Drive, Gmail, and other Google services.

23. Google Android Backup is a service provided by Google Inc. to backup data connected to users' Google accounts. The service allows users to restore data from any Google account that has been backed up in the event that the users' devices are replaced or erased. Data that can be backed up includes Google Calendar settings, WiFi networks and passwords, home screen wallpapers, Gmail settings, applications installed through Google Play, display settings, language and input settings, date and time, and third party application settings and data.

Yahoo Services

24. Oath Holdings Inc. currently operates Yahoo products. Oath Holdings Inc. is a global Internet business and consumer services company headquartered in Sunnyvale, California. It is wholly owned by Verizon Communications. Oath Holdings Inc. offers a comprehensive branded network of properties and services, many of which are free.

25. Yahoo Chat and Yahoo Messenger are two distinct Yahoo products, although users may only access chat rooms via Yahoo Messenger. Yahoo also offers two forms of Messenger – a downloadable client and a version that is accessible on the web. Web-based Messenger may be accessed at messenger.yahoo.com or via Yahoo's new mail interface.

a. For Yahoo Chat and all forms of Messenger, Yahoo has log information regarding the use of the services. Yahoo maintains a "Friends List" for users of Yahoo Messenger and can determine from its logs the times and dates that users logged into Messenger or Chat and the IP addresses used. Yahoo also can retrieve from its Chat and Messenger logs the names of the chat rooms that users accessed and the Yahoo ID's of the other people with whom users communicated through Messenger during the prior 45 to 60 days.

b. For web-based Messenger, Yahoo may be able to access the contents of communications if at least one party to the communications elected to archive the conversation on Yahoo's servers. Yahoo does not archive the contents of communications for the downloadable Messenger client.

26. Flickr is an image hosting and video hosting website and web services suite. It serves as a popular website to share and embed photographs. Images can be uploaded into their sequential "photostream" and displayed in a variety of views, including a justified view, a slideshow, a "detail" view, or a date stamped archive. Clicking on a photostream image opens it in the interactive "photopage" alongside data, comments, and facilities for embedding images on external websites.

a. Users can label their uploaded images with titles and descriptions, and images can be tagged either by the uploader or by other users, if the uploader permits it. These text components enable computer searching of Flickr.

b. Users can organize their Flickr photos into "albums". Flickr provides code to embed albums into blogs, websites, and forums. Geotagging can be applied to photos in albums, and any albums with geotagging can be related to a map using imapflickr. The resulting map can be embedded in a website. Flickr albums may be organized into "collections", which can themselves be further organized into higher-order collections.

c. Organizr is a web application for organizing photos within a Flickr account that can be accessed through the Flickr interface. It allows users to modify tags, descriptions and set groupings, and to place photos on a world map.

27. Yahoo Profiles is a central control panel for online activity, making it easy for people to manage their identities, activities, interests, and connections, and giving users the opportunity to share this information on the web. Each profile includes a basic user card that contains a user's photo (or avatar), nickname, name, age, sex, and location. The profiles also give users the ability to post basic information about their school, work, interests, relationship status, etc. Users will be able to see the other users they are connected to as friends, and there is a section on the profile where a user can see updates from his or her connections. Each profile also includes a "guestbook" where visitors to a profile page can make comments. Yahoo stores the contents of users' current profiles. Yahoo also logs the IP addresses and dates and times of new content added to a profile.

AOL Services

28. Oath Inc. currently operates AOL, formerly known as America Online and AOL Inc. AOL is a web portal and online service provider based in New York that is wholly owned by Verizon Communications. AOL offers a range of integrated products and properties, including dial-up Internet access, AOL Mail (an email service), AOL Instant Messenger

(AIM), and AOL Plans. Oath Inc. currently accepts service of legal process for AOL products at its office location in Dulles, Virginia.

Email Accounts

29. Google allows subscribers to obtain e-mail accounts at the domain name gmail.com, like the accounts listed in Attachment A-1. Yahoo (which is operated by Oath Holdings Inc.) allows subscribers to obtain e-mail accounts at the domain name yahoo.com, like the accounts listed in Attachment A-2. AOL (which is also owned by Oath Inc.) allows subscribers to obtain e-mail accounts at the domain name aol.com, like the accounts listed in Attachment A-3. Subscribers obtain accounts by registering with Google, Yahoo, and AOL. During the registration process, Google, Yahoo, and AOL ask subscribers to provide basic personal information. Therefore, the computers of Google, Yahoo, and AOL are likely to contain stored electronic communications (including retrieved and unretrieved e-mail for Google, Yahoo, and AOL subscribers) and information concerning subscribers and their use of Google, Yahoo, and AOL services, such as account access information, e-mail transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

30. Google, Yahoo, and AOL subscribers can also store with the provider files in addition to e-mails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to e-mails), and other files, on servers maintained and/or owned by Google, Yahoo, and AOL. In my training and experience, evidence of who was using an e-mail account may be found in address books, contact or buddy lists, e-mail in the account, and attachments to e-mails, including pictures and files.

31. E-mail providers generally ask their subscribers to provide certain personal identifying information when registering for an e-mail account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

32. E-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, e-mail providers often have records of the IP address used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the e-mail account.

33. In some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

34. This application seeks a warrant to search all responsive records and information under the control of Google, Oath Holdings Inc., and Oath Inc., providers subject to the jurisdiction of this court, regardless of where Google, Oath Holdings Inc., and Oath Inc. have chosen to store such information. The government intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within Google's, Oath Holdings Inc.'s, and Oath Inc.'s possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States. [1]

35. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the

---

1 It is possible that Google, Oath Holdings Inc., and Oath Inc. store some portion of the information sought outside of the United States. In Microsoft Corp. v. United States, 2016 WL 3770056 (2nd Cir. 2016), the Second Circuit held that the government cannot enforce a warrant under the Stored Communications Act to require a provider to disclose records in its custody and control that are stored outside the United States. As the Second Circuit decision is not binding on this court, I respectfully request that this warrant apply to all responsive information— including data stored outside the United States—pertaining to the identified account that is in the possession, custody, or control of Google, Oath Holdings Inc., and Oath Inc.. The government also seeks the disclosure of the physical location or locations where the information is stored.

geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

Facebook

36. Facebook Inc. owns and operates a free-access social networking website of the same name that can be accessed at http://www.facebook.com. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

37. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers (for password retrieval), physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

38. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "News Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

39. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create "lists" of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

40. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming

"events," such as social occasions, by listing the event's time, location, host, and guest list. In addition, Facebook users can "check in" to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user's profile page also includes a "Wall," which is a space where the user and his or her "Friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

41. Facebook allows users to upload photos and videos, which may include any metadata such as location that the user transmitted when s/he uploaded the photo or video. It also provides users the ability to "tag" (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook's purposes, the photos and videos associated with a user's account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.

42. Facebook users can exchange private messages on Facebook with other users. These messages, which are similar to e-mail messages, are sent to the recipient's "Inbox" on Facebook, which also stores copies of messages sent by the recipient, as well as other information. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a Chat feature that allows users to send and receive instant messages through Facebook. These chat communications are stored in the chat history for the account. Facebook also has a Video Calling feature, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

43. If a Facebook user does not want to interact with another user on Facebook, the first user can "block" the second user from seeing his or her account.

44. Facebook has a "like" feature that allows users to give positive feedback or connect to particular pages. Facebook users can "like" Facebook posts or updates, as well as webpages or content on third-party (*i.e.*, non-Facebook) websites. Facebook users can also become "fans" of particular Facebook pages.

45. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

46. Each Facebook account has an activity log, which is a list of the user's posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as "liking" a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user's Facebook page.

47. Facebook Notes is a blogging feature available to Facebook users, and it enables users to write and post notes or personal web logs ("blogs"), or to import their blogs from other services, such as Xanga, LiveJournal, and Blogger.

48. The Facebook Gifts feature allows users to send virtual "gifts" to their friends that appear as icons on the recipient's profile page. Gifts cost money to purchase, and a personalized message can be attached to each gift. Facebook users can also send each other "pokes," which are free and simply result in a notification to the recipient that he or she has been "poked" by the sender.

49. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

50. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications ("apps") on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user's access or use of that application may appear on the user's profile page.

51. Facebook uses the term "Neoprint" to describe an expanded view of a given user profile. The "Neoprint" for a given user can include the following information from the user's profile: profile contact information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications.

52. Facebook also retains Internet Protocol ("IP") logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user's IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

53. Social networking providers like Facebook typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

54. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user's "Neoprint," IP log, stored electronic communications, and other data retained by Facebook, can indicate who has used or controlled the Facebook account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Facebook logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, Facebook builds geo-location into some of its services. Geo-location allows, for example, users to "tag" their location in posts and Facebook "friends" to locate each other. This geographic and timeline information may tend to either inculpate or exculpate the Facebook account owner. Last, Facebook account activity may provide relevant insight into the Facebook account owner's state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

Cloud Storage and Dropbox

55. Cloud computing has become an increasingly popular way for both individuals and businesses to store and maintain data. Cloud computing utilizes computer resources delivered as a service over a network (typically the Internet). Resources are distributed across a variety of remote data centers in different locations. The following terms relate to the use of cloud computing:

a. "Cloud" is a generic term that refers to a network where the physical location and inner workings are abstracted away and unimportant to the usage. "The cloud" was first used to describe telecommunication networks, where the consumer was blissfully unaware of the inner workings of how their telephone conversation was transmitted to the remote end. The term was later used to describe computer networks, and ultimately to describe the Internet specifically. Knowing the physical location of a website is unimportant to using that service. Cloud computing also takes advantage of this definition of cloud, as it is also a service connected to a network, often the Internet. However, cloud computing offers specific services

whereby customers rent remote computing resources such as processing power or data storage, and provision those resources themselves.

b. "Cloud computing" is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

c. "Cloud Service Provider" (CSP) is the entity that offers cloud computing services. CSP's offer their customers the ability to use infrastructure, platform, or software as a service. These services may include offerings such as remote storage, virtual machines, or Web hosting. Service is billed as a utility based on usage. CSP's maintain records pertaining to the individuals or companies that have subscriber accounts with it. Those records could include identifying and billing information, account access information in the form of log files, account application information, and other information both in computer data format and in written record format. CSP's reserve and/or maintain computer disk storage space on their computer system for the use of the cloud service subscriber for both temporary and long- term storage of electronic data with other parties and other types of electronic data and files. Such temporary, incidental storage is defined by statute as "electronic storage," and the provider of such a service is an "electronic communications service" provider. A cloud service provider that is available to the public and provides long-term storage services to the public for electronic data and files, is providing a "remote computing service." CSP's may be able to provide some of the following, depending on the type of services they provide: NetFlow, Full Packet Captures, Firewall and Router Logs, Intrusion Detection Logs, Virtual Machines, Customer Account Registration, Customer Billing Information.

d. "Virtual Machine" (VM) is a system where the hardware is virtual rather than physical. Virtualization is a technique whereby special software, called the hypervisor, can run many virtual (rather than physical) machines. The hardware on the single machine is emulated so that each virtual instance of a computer, called a VM, does not require dedicated physical hardware, but each VM believes it has its own hardware. The hypervisor has special access to control all of the virtual guests, but it should also be able to isolate the guests from each other.

e. "NetFlow Records" are collections of network statistics collected by a service provider about traffic flows. A traffic flow is a sequence of data packets from a source to a destination. NetFlow is collected when it is impractical to collect all of the data packets for a flow. Providers may use these logs for quality control, security, or billing. For any particular network flow, NetFlow can include the source and destination IP addresses, network ports, timestamps, and amount of traffic transferred. A provider may only collect a sample of all possible sessions, and may only store the NetFlow for a short time.

56. Dropbox is an on-line service that allows its users to store files on Dropbox Inc.'s servers. According to Dropbox Inc.'s privacy policy, at https://www.dropbox.com/privacy, Dropbox Inc. collects and stores "the files you upload, download, or access with the Dropbox Service," and also collects logs: "When you use the Service, we automatically record information from your Device, its software, and your activity using the Services. This may include the Device's IP address, browser type, the web page visited before you came to our website, information you search for on our website, locale preferences, identification numbers associated with your Devices, your mobile carrier, date and time stamps associated with transactions, system configuration information, metadata concerning your Files, and other interactions with the Service.

57. In general, providers like Dropbox Inc. ask each of their subscribers to provide certain personal identifying information when registering for an account. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, e-mail addresses, and, for paying subscribers, a means and source of payment (including any credit or bank account number). Providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the account. In addition, providers often have records of the IP addresses used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account.

58. In some cases, account users will communicate directly with a provider about issues relating to their account, such as technical problems, billing inquiries, or complaints from other users. Providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

Kik Messenger Application

59. Kik is a cross-platform instant messenger application available on smartphones. The application allows users to exchange text-based conversations with one another and to share media such as photos, YouTube videos, and other content.

60. The Kik messenger application is administered by Kik Interactive Inc., a company based in Ontario, Canada. The application can be downloaded free of charge from the Internet. It requires a smartphone with either a data plan or access to a Wi-Fi network to use.

61. Unlike many other smartphone instant messenger applications that are based on a user's telephone number, Kik uses usernames to identify its users. Each user selects and is assigned a unique user name for use on Kik's platform. Each user also creates a user profile, which includes a first and last name and an email address. Kik Interactive Inc. does not verify this information, and as such, users can provide inaccurate information.

62. Kik Interactive Inc. maintains users' profile information and collects IP addresses utilized by users to access the account and transmit messages. In some circumstances, Kik Interactive Inc. also collects users' dates of birth as well as other information about how users have used the messenger application. Kik Interactive Inc. will only release current information to law enforcement pursuant to service of proper legal service (typically profile information and IP addresses for the past thirty days, or the most recent thirty days if the account has not been recently used). Kik Interactive Inc. does not store or maintain chat message content.

63. Based on my training and experience, I know that individuals involved in child pornography offenses often utilize the Kik messenger application to trade child pornography files and to communicate with other offenders and victims. In my experience, a number of child pornography offenders believe that the Kik messenger application is a secure means of trading child pornography.

64. Based on my training and experience, I know that individuals frequently use abbreviations or acronyms when communicating with each other on messenger applications such as Kik. Some of these abbreviations or acronyms include the following (as seen later in the Affidavit):

a. ASAP – As soon as possible

b. HMU – Hit me up

c. IDK – I don't know

d. NVM – Never mind

e. YO – Years old

f. Pics – Pictures

g. Vids - Videos

SextingForum.net Website

65. Based on review of publicly available information, I have learned that an online bulletin board known as SextingForum.Net is located at the website www.sextingforum.net. The bulletin board contains a variety of categories and forums, and it allows users to post messages within these categories and forums. Based on review of the website, much of its content appears to be dedicated to sexually oriented material and the discussion of sexually explicit topics.

66. Review of the SextingForum.net website provided the following information:

a. In order to utilize all of the features available on the website, users need to sign up for a member account. The registration process involves providing an email address and password and establishing an account profile, which includes a user name and gender.

b. The home page for the website is referred to as the "Board Index", and it lists the categories and forums available on the website. The Board Index appears to categorize the forums by the types of social media accounts the users intend to utilize – to include Snapchat, Kik Messenger, WhatsApp, Wicker Messenger, Twitter, and Instagram.

c. Forums are split into various categories. Within each forum, there is a list of topics. Users are able to start new topics within an applicable forum as well as post comments within topics started by others.

d. Next to each post contains information about the user who made the posting. Another user's profile can be viewed by hovering the mouse over the user name.

e. The bulletin board contains a personal messenger application that can be used to exchange private messages with other users.

67. In reviewing reports from other agents and consulting with other investigators from the FBI, I have learned that the SextingForum.net website has been utilized by a number of individuals throughout the United States to obtain, trade, and/or sell child pornography files and to discuss matters related to the sexual abuse of children.

NCMEC and CyberTipline Reports

68. The National Center for Missing and Exploited Children (commonly known as "NCMEC") was founded in 1984 to serve as a clearinghouse on issues related to missing and sexually exploited children. It is currently authorized by Congress to perform 19 programs and

services to assist law enforcement, families, and professions find missing children, reduce child sexual exploitation, and prevent child victimization.

69. As part of its functions, NCMEC administers the CyberTipline. The CyberTipline receives leads and tips from the public and Electronic Service Providers regarding suspected crimes of sexual exploitation committed against children. Electronic Service Providers are required by law to report apparent child pornography to law enforcement via the CyberTipline. Analysts review these tips and refer them to the appropriate federal, state, and local law enforcement authorities.

FACTS SUPPORTING PROBABLE CAUSE

North Carolina Investigation

70. Beginning in 2017, agents and task force officers of the Charlotte (North Carolina) division of the FBI have investigated Andrew Bowles (hereinafter referred to as "Bowles") for child pornography offenses. On or around November 30, 2017, federal search warrants were authorized for Bowles' residence in Benson, North Carolina and for his cellular telephone. The warrants were executed on or around December 6, 2017. Bowles' cellular telephone and various other electronic media were seized pursuant to the warrants. Bowles was interviewed during the execution of the warrants, and he admitted that he viewed and obtained child pornography via a variety of means, including the Kik messenger application. Bowles admitted that his account name on the Kik messenger application was demonelf91. Bowles also admitted that he posted advertisements on the SextingForum.net website, including advertisements related to the sexual exploitation of children.

71. During the subsequent examination of Bowles' cellular telephone, law enforcement officers located messages that Bowles exchanged on the Kik messenger application (using the account name demonelf91) with another individual using the Kik account name of boysunder9. The messages were exchanged on or around August 6, 2017. During the exchange of messages, the boysunder9 account user indicated that he found Bowles' account on the SextingForum.net website. The boysunder9 account user identified that he was 23 years old, lived in Ohio, and had a three-year old nephew. The boysunder9 account user offered to help Bowles have sex with a child. The boysunder9 account user agreed to allow Bowles to have sex with the three-year old nephew, but stated that he wanted something in return. The boysunder9 account user suggested that if Bowles was able to find another child under the age of seven years old, the boysunder9 account user would travel to North Carolina so that he and Bowles could have sex with the three-year old nephew. Specifically, when Bowles offered to allow someone to have sex with him or record his sexual activities, the boysunder9 account user specifically told Bowles that he wanted kids. Below is a transcript of this conversation from the SextingForum.net website:

Boysunder9:	Hey
Demonelf91:	Hello

Boysunder9:	Found you on sexforum
Demonelf91:	Ah. You fit my post or have a lil one?
Boysunder9:	3 nephew
Demonelf91:	3yo?
Boysunder9:	Yes
Demonelf91:	He with you now? Your age?
Demonelf91:	Im a 26yo guy
Boysunder9:	No but I can get him when I want
Boysunder9:	You have any kids
Demonelf91:	No thats why im looking lol.
Demonelf91:	You take any pics of him that I can see? All pics are kept secret between us and never shared
Boysunder9:	Do you know we're any kids live
Demonelf91:	No
Boysunder9:	I'll help you have sex with one and they will stay quiet and not tell
Demonelf91:	With your nephew?
Boysunder9:	What
Demonelf91:	Sex with him
Boysunder9:	No If you get one alone I know what to tell them
Demonelf91:	Im looking for someone that plays with their lil one idk how to get one myself. So can we do it with your nephew or no?
Boysunder9:	Yes
Boysunder9:	I'm wanting something in return
Demonelf91:	I allow someone to have sex with me also or record me no face with him
Boysunder9:	No I want kids
Demonelf91:	Then guess ill keep searching:/
Boysunder9:	I'll help you
Demonelf91:	Okay so youd let me with your nephew?
Boysunder9:	We're you live
Demonelf91:	I'm near Raleigh. You? Your age?
Boysunder9:	We're that
Boysunder9:	23
Demonelf91:	North Carolina.
Demonelf91:	You?
Boysunder9:	Ohio
Demonelf91:	Nvm too far
Boysunder9:	I'll make you a deal
Demonelf91:	?
Boysunder9:	If you get a boy or girl under 7 and Fuck them I'll drive my nephew to you and we will both Fuck him
Demonelf91:	Well no chance on that for me :/
Demonelf91:	Not having luck

Boysunder9:	Do you know any single parents
Demonelf91:	Nope
Boysunder9:	Ok do you know anyone with kids

72. Based on the above noted conversation, I believe that the user of the boysunder9 Kik account had offered to and was attempting to travel in interstate commerce (that being from Ohio to North Carolina) to engage in illicit sexual activity with his three-year old nephew and Bowles.

73. As detailed in the above transcript, the boysunder9 account user indicated that he found Bowles' Kik account on the SextingForum.net website. A law enforcement officer in North Carolina conducted a search of the publicly available information on the SextingForum.net website for the boysunder9 account name. The results of the search indicated that an individual using the Kik account name boysunder9 had posted messages in approximately eight topics. The messages were posted during the approximate time period of May 2017 to October 2017. The individual utilized a user name on the SextingForum.net website of "Bigman23" in the first six postings, "Littledicklover" in the seventh posting, and "Babyboys" in the eighth posting. Below is a summary of these messages from the SextingForum.net website:

a. On or around May 27, 2017, an individual using the account name "Bigman23" started a topic entitled "Trades" in the "Dirty Kik" forum. The "Bigman23" user posted the following:

> "Looking for pics and Vids want to trade boys1-7 and girls 1-4 let me know what you got
> Kik boysunder9"

No one publicly responded to this posting.

b. On or around June 2, 2017, an individual using the account name "Bigman23" started a topic entitled "Parents" in the "Kik Nudes" forum. The "Bigman23" user posted the following:

> "Im looking for anyone who likes to get kids alone and get pics Vids and have fun with them I want to trade mine
> Kik boysunder9"

No one publicly responded to this posting.

c. On or around June 5, 2017, an individual using the account name "Bigman23" responded to a posting made by another individual in a topic entitled "Read" in the "Males Seeking Males" forum. The other individual began the topic by posting the following on or around June 2, 2017:

"Hi. I'm looking for people to trade vids of them fucking their child or wife. I will do the same. But only to the first 5. So hmu asap @paul_tanner"

The Bigman23 user responded on or around June 5, 2017 by stating: "Hey message me on Kik boysunder9".

d. On or around June 10, 2017, an individual using the account name "Bigman23" responded to a posting made by another individual in a topic entitled "Child Porn" in the "Males Seeking Males" forum. The other individual began the topic by posting the following on or around June 8, 2017:

"Send me a full nude pic in the mirror and I will send you child porn Heykyle5"

The Bigman23 user responded on or around June 10, 2017 by stating: "Hey my Kik is boysunder9".

e. On or around June 13, 2017, an individual using the account name "Bigman23" responded to a posting made by another individual in a topic entitled "Got Any Child Porn?" in the "Males Seeking Males" forum. The other individual began the forum by posting the following on or around June 13, 2017:

"Wanna trade child porn? Send porn first for trade back
Add me: akeymon8"

The Bigman23 user responded on or around June 13, 2017 by stating: "Hey message me on Kik. Boysunder9".

f. On or around June 15, 2017, an individual using the account name "Bigman23" started a topic entitled "Parents Or Friends Of Parents For Younger Kids" in the "Dirty Kik" forum. The "Bigman23" user began the topic by posting the following:

"I love to see the little ones played with and made cry I'd love to trade pics and Vids I have my own I'll trade
Kik
Boysunder9"

No one publicly responded to this posting.

g. On or around July 15, 2017, an individual using the account name "Littledicklover" started a topic entitled "Daddy Brother Or Babysitter" in the "Kik Sexting" forum. The "Littledicklover" user began the topic by posting the following:

"Im looking to talk and trade with any one who loves kids
Kik boysunder9"

No one publicly responded to this posting.

h. On or around October 19, 2017, an individual using the account name "Babyboys" started a topic entitled "Child Toddler Baby" in the "Kik Sexting" forum. The "Babyboys" user began the topic by posting the following:

"Wanting to trade I have kids I want to trade pics and videos of to some one who has or can get kids alone
Kik boysunder9
Message me with what you f
Got"

No one publicly responded to this posting.

74. The publicly available information on the SextingForum.net website was reviewed for the "Bigman23", "Littledicklover", and "Babyboys" account profiles. The profile for the "Bigman23" account identified that the user had been a member since on or around May 27, 2017, and was last active on or around June 17, 2017. The gender listed for the user was male. The profile for the "Littledicklover" account identified that the user had been a member since on or around July 15, 2017, and was last active on or around July 19, 2017. The gender listed for the user was female. The profile for the "Babyboys" account identified that the user had been a member since on or around October 18, 2017, and was last active on or around January 3, 2018. The gender listed for the user was female.

75. Based on my training and experience, I know that Kik account names are unique in that only one person can utilize an account name at a time. Given that postings from the "Bigman23", "Littledicklover", and "Babyboys" accounts all identified that the user utilized the Kik account boysunder9, it is reasonable to believe that the three accounts were utilized by the same person.

76. Based on my training and experience, I believe that the postings made by the "Bigman23", "Littledicklover", and "Babyboys" accounts (as detailed above) are consistent with individuals who are attempting to obtain and trade child pornography files with others. For example, two of the topics that the "Bigman23" account user responded to were explicitly entitled "Child Porn" and "Got Any Child Porn". Also for example, the title of one of the topics posted by the "Babyboys" account user reflected the apparent desired ages of children – "Child Toddler Baby". Based on all of the information noted in the Affidavit, I submit that it is reasonable to believe that by posting the information noted above on the SextingForum.net website, the boysunder9 account user was: (1) attempting to receive and possess child pornography, and (2) making, printing, or publishing advertisements to receive and/or exchange child pornography files with others.

77. Also based on my training and experience, I believe that the postings made by the "Bigman23", "Littledicklover", and "Babyboys" accounts are indicative of someone who possesses a collection of child pornography. For example, on June 2, 2017, the "Bigman23" account user stated "I'd love to trade pics and vids I have my own I'll trade". Also for example, on June 15, 2017, the "Bigman23" account user stated "I want to trade mine".

Service of Subpoenas and Review of Other Records

78. During the course of the investigation, two administrative subpoenas were served to Kik Interactive Inc. requesting subscriber information for the boysunder9 account, as well as logs of IP addresses utilized to access the account and transmit messages. The subpoenas were served to Kik Interactive Inc. on or around January 22, 2018 and February 5, 2018. The records from Kik Interactive Inc. provided the following information:

a. The boysunder9 account was created on or around January 22, 2017. The profile name for the account was "John Adams", and the email address **lovepics9@yahoo.com** was associated with the account profile.

b. The account was last accessed on or around December 5, 2017. The IP address of 107.198.170.99 was used to access the account on this date. No other IP addresses were provided by Kik Interactive Inc., as prior activity was beyond the standard 30-day period of which Kik Interactive Inc. will release records pursuant to a subpoena (as detailed above).

c. A ZTE Model N9519 android device was used to access the account on or around December 4, 2017.

79. AT&T was identified as the service provider for the IP address: 107.198.170.99. On or around January 29, 2018, an administrative subpoena was served to AT&T requesting subscriber information for this IP address on December 5, 2017 at the approximate time it was used to access the boysunder9 Kik account. Records received in response to the subpoena identified that the IP address was subscribed to TYLER ULM at 305 East Maplewood Avenue, Dayton, Ohio. AT&T's records identified that TYLER ULM's telephone number was 937-931-1151. Records identified that the Internet account was activated on or around November 25, 2017, and that it was active as of the date of the subpoena.

80. Sprint was identified as the service provider for telephone number 937-931-1151. On or around February 6 and 7, 2018, administrative subpoenas were served to Sprint requesting subscriber information and device information for this telephone number. Records received in response to the subpoenas identified that the telephone number was subscribed to TYLER ULM at 305 East Maplewood Avenue, Dayton, Ohio. According to Sprint's records, the device that utilized this telephone number was a Boost ZTE Model N9519 cellular telephone. As detailed above, this same make and model of cellular telephone was utilized

to access the boysunder9 Kik account on or around December 4, 2017.

81. On or around February 5, 2018, an administrative subpoena was served to Yahoo Holdings Inc. requesting subscriber information for the email address **lovepics9@yahoo.com** (the email address associated with the boysunder9 Kik account) and logs of IP addresses utilized to access the account. Records received from Yahoo Holdings Inc. in response to the subpoena identified that the account was created on or around January 12, 2017 in the name of "John Adams". Telephone number 937-931-1151 (the telephone number subscribed to TYLER ULM, as detailed above) was listed as an alternate communication channel for the account. The records indicated that this telephone number had been verified by Yahoo Holdings Inc. The email account was deactivated on or around May 5, 2017.

82. On or around February 8, 2017, an administrative subpoena was served to Charter Communications requesting subscriber information for a sample of four of the IP addresses utilized to log into the **lovepics9@yahoo.com** account (as identified in the logs of IP addresses provided by Yahoo Holdings Inc.). Records received in response to the subpoena identified that each of these IP addresses were subscribed to Jacqueline Ulm at 305 East Maplewood Avenue, Dayton, Ohio. Based on information from a prior report of the Dayton Police Department, it appears that Jacqueline Ulm is TYLER ULM's mother.

83. Review of records from the Ohio Bureau of Motor Vehicles identified that TYLER ULM utilized the address of 305 East Maplewood Avenue, Dayton, Ohio, on his current Ohio driver's license. The driver's license identified that TYLER ULM is presently 23 years old (consistent with the age provided by the boysunder9 account user in his communications with Bowles).

84. In reviewing publicly accessible data on the Facebook website, I located an account in the name of TYLER ULM and a Facebook user ID of **Tyler.Ulm.7** (located at https://wwww.facebook.com/tyler.ulm.7). Based on review of photographs and other data for the account, this individual appears to be the same TYLER ULM who utilized the address of 305 East Maplewood Avenue, Dayton, Ohio on his current Ohio driver's license. The publicly available data contained on the account included approximately nine photographs that depicted a juvenile boy sitting on the lap of TYLER ULM. The juvenile boy appears to be approximately two to four years old (consistent with the age of the nephew that the boysunder9 account user identified as having in his communications with Bowles).

Cyber Tipline Reports

85. As part of the investigation, I learned that Yahoo has made four reports to NCMEC's CyberTipline regarding suspected child pornography files located in Flickr accounts associated telephone number 937-931-1151 (the telephone number subscribed to TYLER ULM and listed as an alternate communication channel for the **lovepics9@yahoo.com** email address, as detailed above) and/or the name of "John Adams". These four reports were made during the time period of December 2016 to December 2017. NCMEC forwarded the

four reports, along with the suspected child pornography files that were provided by Yahoo, to the Ohio Internet Crimes Against Children Task Force (ICAC) for further investigation. I have obtained and reviewed these reports and suspected child pornography files from the Cuyahoga County ICAC as part of the current investigation.

86. On or around December 15, 2016, Yahoo reported to NCMEC's CyberTipline that a suspected child pornography file was located in a Flickr account bearing NSID[2] **146969803@N06**, which was associated with the email address **d9underboy@yahoo.com**. Yahoo provided the following information to NCMEC regarding these accounts:

a. The email account **d9underboy@yahoo.com** was created on or around December 7, 2016. When opening the account, the account user provided a name of "John Adams", a gender of female, and a date of birth of January 1, 1990.

b. An associated Flickr account in the name "John Adams2016" was created on or around December 6, 2016. The Flickr account had a display name of "John Adams" and a Flickr NSID of **146969803@N06.** The URL for the account was https://www.flickr.com/photos/146969803@N036.

c. Telephone number 937-931-1151 was associated with the account. Yahoo's records indicated that a representative verified that this telephone number was accurate on or around December 7, 2016.

d. Yahoo deactivated the account on or around December 15, 2016, after finding one suspected child pornography file in the Flickr account. I have reviewed the file, and based on my training and experience, I believe that it depicts child pornography (as defined in 18 U.S.C. § 2256). The file is described as follows:

i. img.3-1.jpg: The file is a close-up image of the nude penis of what appears to be a toddler-aged male child. The hand of another individual is touching the child's penis.

87. On or around December 30, 2017, Yahoo reported to NCMEC's CyberTipline that suspected child pornography files were located in a Flickr account bearing NSID **150137400@N03**, which was associated with the email address **kids9nunder@yahoo.com**. Yahoo provided the following information to NCMEC regarding these accounts:

a. The email account **kids9nunder@yahoo.com** was created on or around December 17, 2016. When opening the account, the account user provided a name of "Tom Adams", a gender of female, and a date of birth of June 1, 1969.

b. An associated Flickr account in the name "Tom Adams2016" was created on or

2 NSID's are user identification numbers for Flickr accounts.

around December 17, 2016. The Flickr account had a display name of "Tom Adams" and a Flickr NSID of **150137400@N03**. The URL for the account was https://www.flickr.com/photos/150137400@N03.

c. Telephone number 937-931-1151 was associated with the account. Yahoo's records indicated that a representative verified that this telephone number was accurate on or around December 29, 2016.

d. Yahoo deactivated the account on or around December 29, 2016, after finding approximately five suspected child pornography files in the account. I have reviewed the five files, and based on my training and experience, I believe that they depict child pornography (as defined in 18 U.S.C. § 2256). By way of example, one of the files is described as follows:

i. **img.5-1**: The file is an image that depicts a nude infant or toddler-aged male child lying on his back with his legs spread apart, exposing his nude penis to the camera.

88. As part of reporting the Flicker NSID's **146969803@N06** and **150137400@N03** to NCMEC's CyberTipline in December 2016, Yahoo also provided information regarding two other accounts that appeared to be used by the same person: **littleboysunder@yahoo.com** and **tylerjulm@yahoo.com**. Yahoo provided the following information to NCMEC regarding the **littleboysunder@yahoo.com** account as part of their CyberTipline reports in December 2016:

a. The email account **littleboysunder@yahoo.com** was created on or around November 28, 2016. When opening the account, the account user provided a name of "John Adams", a gender of female, and a date of birth of January 1, 1998.

b. An associated Flickr account in the name "johnadams19" was created on or around November 28, 2016. The Flickr account had a display name of "John Adams" and a Flickr NSID of **146772605@N03**. The URL for the account was https://www.flickr.com/photos/146772605@N03.

c. Telephone number 937-931-1151 was associated with the account. Yahoo's records indicated that a representative verified that this telephone number was accurate on or around December 29, 2016.

89. Yahoo provided the following information to NCMEC regarding the **tylerjulm@yahoo.com** account as part of their CyberTipline reports in December 2016:

a. The email account **tylerjulm@yahoo.com** was created on or around July 22, 2016. When opening the account, the account user provided a name of "Tayler Hom", a gender of female, and a date of December 1, 1990.

b. An associated Flickr account in the name **"Tayler Hom"** was created on or around July 22, 2016. The Flickr account had a display name of "Tayler Hom" and a Flickr NSID of **145287374@N02**. The URL for the account was https://www.flickr.com/photos/145287374@N02.

c. Telephone number 937-931-1151 was associated with the account. Yahoo's records indicated that a representative verified that this telephone number was accurate on or around November 28, 2016.

90. On or around January 17, 2017, Yahoo reported to NCMEC's CyberTipline that suspected child pornography files were located in a Flickr account bearing NSID **147418551@N04.** Yahoo provided the following information to NCMEC regarding this account:

a. The Flickr account was in the name of "Love Pics".

b. The Flickr account was associated with the email address **omkexddwbkit3s2eatevv5zx3bne75kjo4kfarxo@yahoo.com**.

c. Telephone number 937-931-1151 was associated with the account.

d. Yahoo found approximately three suspected child pornography files in the Flickr account. I have reviewed the three files, and based on my training and experience, I believe that they depict child pornography (as defined in 18 U.S.C. § 2256). By way of example, one of the files is described as follows:

i. **img.4-1**: The file is an image that depicts a nude infant or toddler-aged male child lying on his back with his legs spread apart, exposing his nude penis to the camera.

91. On or around December 19, 2017, Yahoo reported to NCMEC's CyberTipline that a suspected child pornography file was located in a Flickr account bearing NSID **161195535@N07.** Yahoo provided the following information to NCMEC regarding this account:

a. The Flickr account was in the name of "John Adams".

b. The Flickr account was associated with the email address legal-cpr@yahoo-inc.com.

c. No telephone number was provided for the account. The email address **lovepics9@aol.com** was listed as an alternate communication channel for the account.

d. Yahoo found approximately one suspected child pornography file in the Flickr account. I have reviewed the file, and based on my training and experience, I believe

that it depicts child pornography (as defined in 18 U.S.C. § 2256). The file is described as follows:

i. Img.1-1.jpg: The file is an image that depicts two nude pre-pubescent male children and one nude pre-pubescent female child in a bathroom. The penis and vagina of two of the children are exposed to the camera.

92. Given that the six accounts reported by Yahoo to NCMEC's CyberTipline were all associated with telephone number 937-931-1151 and/or contained a user name of "John Adams", it is reasonable to believe that they were utilized by the same person.

Execution of Search Warrants

93. On February 14, 2018, search warrants were authorized by the United States District Court for the Southern District of Ohio for (1) the residential property located at 305 East Maplewood Avenue, Dayton, Ohio, and (2) the person of TYLER ULM. Agents and officers of the FBI and Dayton Police Department executed the warrants on February 15, 2018. An adult female who will be referred to for purposes of this Affidavit as "Female A" was present when agents and officers arrived. Various electronic media were located in the residence and seized pursuant to the search warrant.

94. During the execution of the search warrant for the residence, Female A agreed to be interviewed. In summary, Female A provided the following information during the interview:

a. TYLER ULM was Female A's boyfriend. They lived together at 305 East Maplewood Avenue, Dayton, Ohio.

b. Female A stated that she had never used the Kik Messenger application or the SextingForum.net website. TYLER ULM had utilized a Kik account in the past, but Female A did not know his account name or if he still utilized the account.

c. Female A stated that she did not use the email account **lovepics9@yahoo.com** and did not know anyone who used this account. Female A also stated that she did use the account names "boysunder9", "Bigman23", "Littledicklover", or "Babyboys", and she did not know anyone who used these account names.

d. Female A had a nephew who was two years old.

95. Also during the execution of the search warrant for the residence, a 1997 Dodge Grand Caravan vehicle that was registered to Female A arrived and parked a short distance away from the residence. TYLER ULM was in the passenger seat of the vehicle, and a man who identified himself as TYLER ULM's father was in the driver's seat. TYLER ULM got out of the vehicle as agents and officers approached him. His person was searched pursuant to the search warrant, and no items of evidence were seized.

96. Officers observed a cellular telephone between the front seats of the 1997 Dodge Grand Caravan vehicle (within arm's reach of where TYLER ULM was sitting when he arrived). Female A provided her written consent for agents and officers to search the vehicle. An officer thereafter searched the vehicle and seized a ZTE cellular telephone bearing Model N9519 and serial number 320375817555. It was noted that this telephone is the same make and model of cellular telephone that was utilized to access the boysunder9 Kik account on or around December 4, 2017 (as detailed above).

97. TYLER ULM agreed to be interviewed after being advised of his Miranda rights. In summary, TYLER ULM provided the following information during the interview:

a. TYLER ULM resided at 305 East Maplewood Avenue, Dayton, Ohio, with Female A. His mother previously resided at the residence as well, but she died a few days prior.

b. The ZTE cellular telephone seized from the Dodge Grand Caravan is TYLER ULM's cellular telephone, and his cellular telephone number is 937-931-1151 (the number listed as an alternate communication channel for the **lovepics9@yahoo.com** email account and three of the accounts reported by Yahoo to NCMEC's CyberTipline, as detailed above).

c. TYLER ULM stated that he utilized the email accounts **tylerjulm22@gmail.com** and **tylerjulm@gmail.com**. He denied utilizing any other email accounts within the past approximately six years.

d. TYLER ULM denied ever using the Kik Messenger application.

e. TYLER ULM denied using any Dropbox accounts.

f. TYLER ULM stated that he did not use the email account **lovepics9@yahoo.com** and did not know anyone who used this account. TYLER ULM also stated that he did use the account names "boysunder9", "Bigman23", "Littledicklover", or "Babyboys", and he did not know anyone who used these account names.

g. TYLER ULM did not have any biological nephews. However, TYLER ULM had been around the children of some of his friends. These children included three boys who were approximately two to four years old.

h. TYLER ULM stated that there had been times when he fantasized about children and talked about these fantasies with others, but that he never engaged in sexual activities with children. TYLER ULM then terminated the interview.

98. On February 16, 2018, a search warrant was authorized by the United States District Court

for the Southern District of Ohio for TYLER ULM's ZTE Model N9519 cellular telephone. A preliminary review of the telephone has been conducted at this time. The following information was obtained during the preliminary review:

a. To date, at least approximately twenty image files depicting child pornography (as defined in 18 U.S.C. § 2256) have been recovered from the telephone. Based on file property information, it appears that these images were created on the telephone on approximately four dates during the approximate time period of October 19, 2017 to November 22, 2017. By way of example, two of the files are described as follows:

   i. 1508800134390.jpg: The file is a close-up image of a pre-pubescent male child with his legs spread apart. The penis of what appears to be an adult male is partially inserted into the child's anus.

   ii. 1511307440291.jpg: The file is an image that depicts two nude pre-pubescent male children lying on a bed together. The penis of one of the children is in the mouth of the other child.

b. Contrary to TYLER ULM's statements, a user account[3] was established on the telephone for an account on the Kik website on or around May 4, 2017. The information available on the telephone did not include the account name but identified that the password for the account was boysunder9. The Kik application was not currently installed on the telephone. As such, communications on the Kik messenger application utilizing the user account have not been recovered from the telephone as of this time.

c. Also contrary to TYLER ULM's statements, the email address **lovepics9@yahoo.com** was saved as a user account on the telephone. On or around May 4, 2017, another user account was established on the telephone for an account on the SexForums.com website (a website for chatting about sexually explicit topics and exchanging nude or sexually-explicit photographs). The user name for the account was **lovepics9@yahoo.com**, and the password was boysunder9.

d. Four user accounts were established on the telephone for accounts on the SextingForum.net website: (1) an account with a user name of **johnadams1.9@yahoo.com** and password of boysunder8, established on or around May 18, 2017; (2) an account with a user name of boysunder9@yahoo.com and password of boysunder4, established on or around July 15, 2017 (the same date that the "Littledicklover" account was created, as detailed above); (3) an account with a user name of tylerulm@yahoo.com and password of boysunder9, established on or around August 30, 2017; and (4) an account with a user name of

---

3 On many Android cellular telephones such as the ZTE telephone seized pursuant to the search warrant, users can set up various user accounts on the phone for email and social media accounts they commonly utilize. These user accounts are stored in the phone's settings.

D9boylover@yahoo.com and password of boysunder9, established on or around October 18, 2017 (the same date that the "Babyboys" account was created, as detailed above).

i. Based on information provided by Yahoo, the email addresses boysunder9@yahoo.com, tylerulm@yahoo.com, and D9Boylover@yahoo.com are not currently open email addresses. Based on my review of the SextingForum.net website, I know that accounts can be created on this website using fictitious email addresses.

e. On or around January 3, 2017, a user account was established on the telephone for an account on the Yandex website. The user name for this account was Littleboysunder, and the password was boysunder9.

i. Based on my training and experience, I know that Yandex is a multinational technology company specializing in Internet-related products and services. Although most of its assets are in Russia, its headquarters is in the Netherlands. Among other products and services, Yandex provides users with email service, a web browser, a search engine, and cloud storage. Based on my training and experience, I know that Yandex's products (to include email and cloud storage) have been utilized by child pornography offenders to store and trade child pornography files.

f. The email addresses **tylerjulm22@gmail.com** and **tylerjulm@gmail.com** were established as user accounts on the telephone. As noted above, TYLER ULM identified during the interview that he used these two email accounts. The telephone's data identified that Google+ and Google Drive accounts existed for the two email addresses. The telephone's data also indicated that more than 600 image files had been saved to a Google Drive account associated with the email address **tylerjulm22@gmail.com**.

g. On or around November 11, 2016, a user account was established on the telephone for an account on the Live.com website (a website associated with Microsoft accounts). The user name for this account was **damonvaughn0@gmail.com**.

h. On or around October 15, 2016, a user account was established on the telephone for an account on the Netflix website (a website that allows users to watch television shows and movies online). The user name for this account was **ahopping0406@aol.com**.

i. On or around July 15, 2017, a user account was established on the telephone for an account on the Dropbox website. The user name and password for the account were not saved in the telephone's data.

j. On or around January 27, 2017, a user account was established on the telephone for an account on the Facebook website. The account had a user name of 9379311151.

i. I conducted a search of the publicly available content on the Facebook website for accounts associated with telephone number 937-931-1151. I found that the **Tyler.Ulm.7** account (the account identified above in paragraph 84) is associated with this telephone number.

Identification of Dropbox Accounts

99. On or around February 22, 2018, Dropbox Inc. was served with an administrative subpoena requesting subscriber information for any accounts associated with email addresses suspected to be utilized by TYLER ULM (as detailed above) as well as the logs of IP addresses utilized to access these accounts during the time period of January 1, 2017 to February 22, 2018. In response to the subpoena, Dropbox Inc. provided records for four accounts associated with the following email addresses: **littleboysunder@yahoo.com**, **lovepics9@yahoo.com**, **lovepics9@aol.com**, and **johnadams1.9@yahoo.com**. The subscriber information provided by Dropbox Inc. identified that all of the accounts were created in the name of "John Adams". The records from Dropbox Inc. provided the following information:

a. On or around December 8, 2016, a Dropbox account was created in the name of "John Adams", utilizing an email address of **littleboysunder@yahoo.com**. The logs of IP addresses identified that the account was last logged into on or around December 25, 2017. Dropbox Inc.'s records identified that a Boost Mobile Model N9519 cellular telephone (consistent with TYLER ULM's telephone) had been utilized to access the account on approximately fifty-six occasions. Although the Boost Mobile Model N9519 cellular telephone was primarily utilized to access the account, several other cellular telephones also accessed the account.

b. On or around January 28, 2017, a Dropbox account was created in the name of "John Adams", utilizing an email address of **lovepics9@yahoo.com**. The logs of IP addresses identified that the account was last logged into on or around February 13, 2018. Dropbox Inc.'s records identified that a Boost Mobile Model N9519 cellular telephone (consistent with TYLER ULM's telephone) had been utilized to access the account on approximately forty-five occasions. Although the Boost Mobile Model N9519 cellular telephone was primarily utilized to access the account, several other cellular telephones also accessed the account.

c. On or around November 20, 2017, a Dropbox account was created in the name of "John Adams", utilizing an email address of **lovepics9@aol.com**. The logs of IP addresses identified that the account was last logged into on or around January 17, 2018. Dropbox Inc.'s records identified that a Boost Mobile Model N9519 cellular telephone (consistent with TYLER ULM's telephone) had been utilized to access the account on approximately twelve occasions. No other model of cellular telephones

was utilized to access this account.

d. On or around May 12, 2017, a Dropbox account was created in the name of "John Adams", utilizing an email address of **johnadams1.9@yahoo.com**. The logs of IP addresses identified that the account was last logged into on or around December 25, 2017. Dropbox Inc.'s records identified that a Boost Mobile Model N9519 cellular telephone (consistent with TYLER ULM's telephone) had been utilized to access the account on approximately fifty-three occasions. Although the Boost Mobile Model N9519 cellular telephone was primarily utilized to access the account, several other cellular telephones also accessed the account.

100. Based on the information detailed above, it appears that the four previously noted Dropbox accounts were used by an individual who utilized a Boost Mobile Model N9519 cellular telephone. Based on my training and experience, I know that individuals often create sharing links to their Dropbox accounts in order to share files with others. Based on the fact that more than one cellular telephone accessed three of the four Dropbox accounts detailed above, it appears that the user of the three accounts created sharing links to his account.

Conclusion Regarding Use of Accounts

101. As detailed above, TYLER ULM denied that he utilized any Kik accounts, any email accounts other than **tylerjulm22@gmail.com** and **tylerjulm@gmail.com**, and any Dropbox accounts. Based on my training and experience, I know that individuals involved in child exploitation activities often attempt to conceal the accounts they utilize to carry out their criminal activities.

102. Based on all of the information detailed in this Affidavit, there is probable cause to believe that TYLER ULM is the user of the following accounts:

a. The boysunder9 Kik account;

b. The "Bigman23", "Littledicklover", and "Babyboys" accounts on the SextingForum.net website;

c. The **tylerjulm22@gmail.com**, **tylerjulm@gmail.com**, and **damonvaughn0@gmail.com** Google Accounts;

d. The **lovepics9@yahoo.com**, **d9underboy@yahoo.com**, **kids9nunder@yahoo.com**, **littleboysunder@yahoo.com**, **johnadams1.9@yahoo.com**, **tylerjulm@yahoo.com**, and **omkexddwbkit3s2eatevv5zx3bne75kjo4kfarxo@yahoo.com** Yahoo email accounts;

e. The Flickr accounts associated with the Flickr NSID's **146969803@N06, 150137400@N03, 146772605@N03, 145287374@N02, 161195535@N07,** and **147418551@N04**;

f. The **ahopping0406@aol.com** and **lovepics9@aol.com** AOL accounts;

g. The **Tyler.Ulm.7** Facebook account; and

h. The Dropbox accounts associated with the email addresses **littleboysunder@yahoo.com, lovepics9@yahoo.com, lovepics9@aol.com**, and **johnadams1.9@yahoo.com**

103. There is also probable cause to believe that TYLER ULM has utilized at least some of the above noted accounts to possess or attempt to possess child pornography, receive or attempt to receive child pornography, advertise child pornography, and attempt to travel in interstate commerce with the intent to engage in illicit sexual conduct.

104. Based on my training and experience, I know that individuals involved in child exploitation offenses and other criminal activities often utilize fictitious names and identifying information (to include gender and age) when registering the online accounts they utilize in the commission of the criminal activities. Individuals utilize fictitious names and identifying information as a means to avoid detection and evade law enforcement officers. Also based on my training and experience, I know that individuals involved in child exploitation offenses sometimes utilize multiple aliases as a means to obtain more trading partners and/or gain access to more victims. Given the use of fictitious names and/or gender when registering the boysunder9 Kik account, the "Littledicklover" and "Babyboys" accounts on the SextingForum.net website, and the various Yahoo email accounts, it appears that TYLER ULM utilized fictitious names and/or multiple aliases.

Evidence Available on Email and Social Media Accounts

105. Based on my training and experience, I am aware that individuals involved in child exploitation schemes often communicate with others involved in similar offenses about their victims and sexual activities via e-mail, social media accounts such as Google+ and Facebook, and online chat programs such as Yahoo Chat and Messenger. I have seen examples of cases where such individuals have communicated with other child predators about their sexual fantasies and prior sexual activities with juveniles. I have also seen cases where such individuals have communicated with others about their remorse and regret for their activities. Both types of communications provide material evidence in child exploitation cases in that they provide admissions of guilt.

106. Also in my experience, individuals involved in child exploitation schemes often utilize social media accounts such as Google+ and Facebook and other websites as a means to locate and recruit victims. They then use the chat functions on these and other websites, as

well as email accounts, to communicate with their victims. Such communications provide a means of anonymity to protect the subjects' identities and to conceal the communications from the victims' parents.

107. Based on my training and experience, I know that individuals involved in child pornography offenses often obtain and trade images with each other via a variety of means, including email, social media accounts such as Facebook and Google+, photo sharing services such as Google Photos and Flickr, and online chat programs such as Yahoo Messenger. Individuals also often attempt to obtain child pornography from a variety of sources, including from those with whom they communicate via email, social media sites, Internet chat programs, Internet bulletin boards, Internet Peer-to-Peer file sharing programs, Internet websites, and other sources. I have also seen a number of cases in which individuals email files containing child pornography to themselves – either from one email account to another or from and to the same email account – in order to transfer the files from one electronic device to another.

108. Based on my training and experience, one or more aliases are often used by individuals involved in child exploitation offenses as a means to avoid detection from law enforcement. It is not uncommon for such offenders to create multiple identities, sometimes involving different ages and genders. Offenders sometimes fictitiously portray themselves as juveniles as a means to gain trust and rapport with victims. Offenders also sometimes obtain photographs of other individuals from the Internet to use as their profile pictures and/or to send to the victims.

109. Based on my training and experience, I know that many social media accounts and Internet websites require users to provide their email account when registering for the accounts. The social media account providers and Internet providers then send the users various notifications regarding messages from other users, information accessed by users, information available by the websites, and other information. These messages can provide material evidence in cases involving child exploitation offenses because they help in identifying what social media and Internet accounts were utilized by the subjects to communicate with other subjects and victims and what accounts were utilized by the subjects to find child pornography. In addition, the messages help in identifying the identities of other subjects and victims.

110. Also based on my training and experience, I know that individuals frequently post photographs of themselves and their family members and friends on their social media accounts and photo sharing services such as Google Photos and Flickr. These photographs often depict a variety of settings and sometimes reflect their whereabouts. Individuals also often post written information to their timelines that identifies their whereabouts. In cases where engage in or attempt to engage in sexually explicit conduct with children, the innocuous photographs and postings contained on the offenders' social media accounts may be materially relevant in determining the identities of the victims and the locations where the sexual activities took place.

111. Indicia of travel that subjects took to engage in criminal sexual activities may be found in various other forms, to include receipts for purchases of gasoline, hotel receipts and invoices, receipts for purchases of food and other items, checking account statements, credit card statements, and various financial documents. The financial documents such as checking account statements and credit card statements may also provide evidence of items subjects purchased during the travels. Based on my training and experience, I know that hotels, financial institutions, and various stores sometimes email these types of documents to their customers.

112. Also as noted above, email providers maintain various subscriber and user information that its users provide when registering for its accounts. Some email providers also require payment for certain services or features. Such information is materially important in cases where online accounts are utilized to trade child pornography, as this information can help in confirming the identities of the individuals using the accounts and committing the offenses.

113. As detailed above, Yahoo Profiles may contain account profile pictures and other identifying information for the users. This information may be materially relevant in investigations where individuals utilize Yahoo accounts to conduct child exploitation activities because it may help confirm the identities of the account users and/or provide information about the account users' aliases.

114. Email providers maintain various logs of IP addresses utilized to access the accounts. The IP information is again materially important in child pornography investigations. This information helps in identifying the subjects and the locations where their computer devices are located.

Evidence Available on Other Google and Yahoo Accounts

115. Google has the ability to maintain information associated with the Web and Application history of its users. Such information is materially relevant in child exploitation investigations, as it may help in identifying websites used by subjects to obtain child pornography and locate victims. In addition, in cases involving subjects who travel or attempt to travel to engage in criminal sexual activities, the Web and Application history maintained by Google may also provide evidence of the Internet searches subjects conduct to obtain directions to the locations of the criminal activities.

116. Google Drive, Google Photos, and Flickr provide users with cloud computing and online file storage (as detailed above) and photo storage services. In my experience, individuals with large collections of child pornography may utilize cloud computing and online storage accounts as a means to store their files after their hard drives become full. In addition, individuals utilize these services as a means to conceal their files from others, including law enforcement.

117. Google Android Backup provides users with the ability to backup data on their cellular telephones and other electronic devices. Such data can be materially relevant in cases in

which cellular telephones and other electronic devices are used to commit child exploitation offenses, as this data may provide historical records of their criminal activities that are no longer saved on the devices.

Evidence Available on Dropbox Accounts

118. Dropbox and other cloud storage services provide a means that individuals can use to store files. In my experience, individuals with large collections of child pornography may utilize cloud computing and online storage accounts as a means to store their files after their hard drives become full. In addition, individuals utilize these services as a means to conceal their files from others, including law enforcement.

119. Based on information received from Dropbox Inc., I know that Dropbox Inc. maintains basic subscriber information for its users, including user names, email addresses, and the dates that they established their accounts. Dropbox Inc. also maintains payment information, including credit card numbers, when payments are made on the accounts. Such information can provide material evidence regarding individuals involved in child pornography offenses, because this information can help identify the subjects and determine what aliases and email accounts they utilize. In addition, the dates that the accounts were established can help in identifying the length of time that the criminal activities transpired.

120. In addition to maintaining the files themselves, Dropbox Inc. also maintains files documenting various activities associated with its accounts. One such file is entitled "uploadlog.html". This file maintains information about the account name, computer name, and dates that files were uploaded, deleted, and modified. Such information provides material evidence to child pornography investigations, as the information helps identify the computer devices utilized by the subjects and when and how the files were received.

121. Another file maintained by Dropbox Inc. for its accounts is entitled "auth.txt". This file maintains logs of IP addresses and devices utilized to access the account. Such information is important to child pornography investigations because it helps to establish the subjects' identities, what computer devices are utilized, where the subjects' computers are located, and when the criminal activities transpired.

122. A file entitled "links.txt" is another example of a file maintained by Dropbox Inc. for its accounts. This file maintains information about files being shared by the user. In cases involving the trading of child pornography, information about the shared files can be useful in helping to identify the subjects' trading activities.

123. Dropbox Inc. maintains various information about the settings for its users' accounts. Such settings include information about computers and other devices linked to the accounts. Information about what computers and devices are utilized by the subjects is again materially important to child pornography investigations.

ELECTRONIC COMMUNICATIONS PRIVACY ACT

124. I anticipate executing the requested warrants for the listed accounts under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrants to require Google Inc., Oath Holdings Inc., Oath Inc., Facebook Inc., and Dropbox Inc. to disclose to the government copies of the records and other information (including the contents of communications) particularly described in Section I of Attachments B-1 through B-5. Upon receipt of the information described in Section I of Attachments B-1 through B-5, government-authorized persons will review that information to locate the items described in Section II of Attachments B-1 through B-5.

CONCLUSION

125. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence, fruits, and instrumentalities of the following criminal offenses may be located in the accounts described in Attachments A-1 through A-5: 18 U.S.C. §§ 2252(a)(4)(B) and (b)(1) and 2252A(a)(5)(B) and (b)(1), which make it a crime to possess or attempt to possess child pornography; violations of 18 U.S.C. §§2252(a)(2)(B) and (b)(1) and 2252A(a)(2) and (b)(1), which make it a crime to receive or attempt to receive child pornography through interstate commerce; violations of 18 U.S.C. §2251(d), which make it a crime to advertise child pornography; and violations of 18 U.S.C. §2423(b) and (e), which make it a crime to travel or attempt to travel in interstate commerce with the intent to engage in illicit sexual conduct.

126. I, therefore, respectfully request that the attached warrants be issued authorizing the search and seizure of the items listed in Attachments B-1 through B-5.

127. Because the warrants for the accounts described in Attachments A-1 through A-5 will be served on Google Inc., Oath Holdings Inc., Oath Inc., Facebook Inc., and Dropbox Inc., who will then compile the requested records at times convenient to those entities, reasonable cause exists to permit the execution of the requested warrants at any time in the day or night.

Special Agent Andrea R. Rinzig
Federal Bureau of Investigation

SUBSCRIBED and SWORN
before me this 2nd of March 2018

Sharon L. Ovington
UNITED STATES MAGISTRATE JUDGE